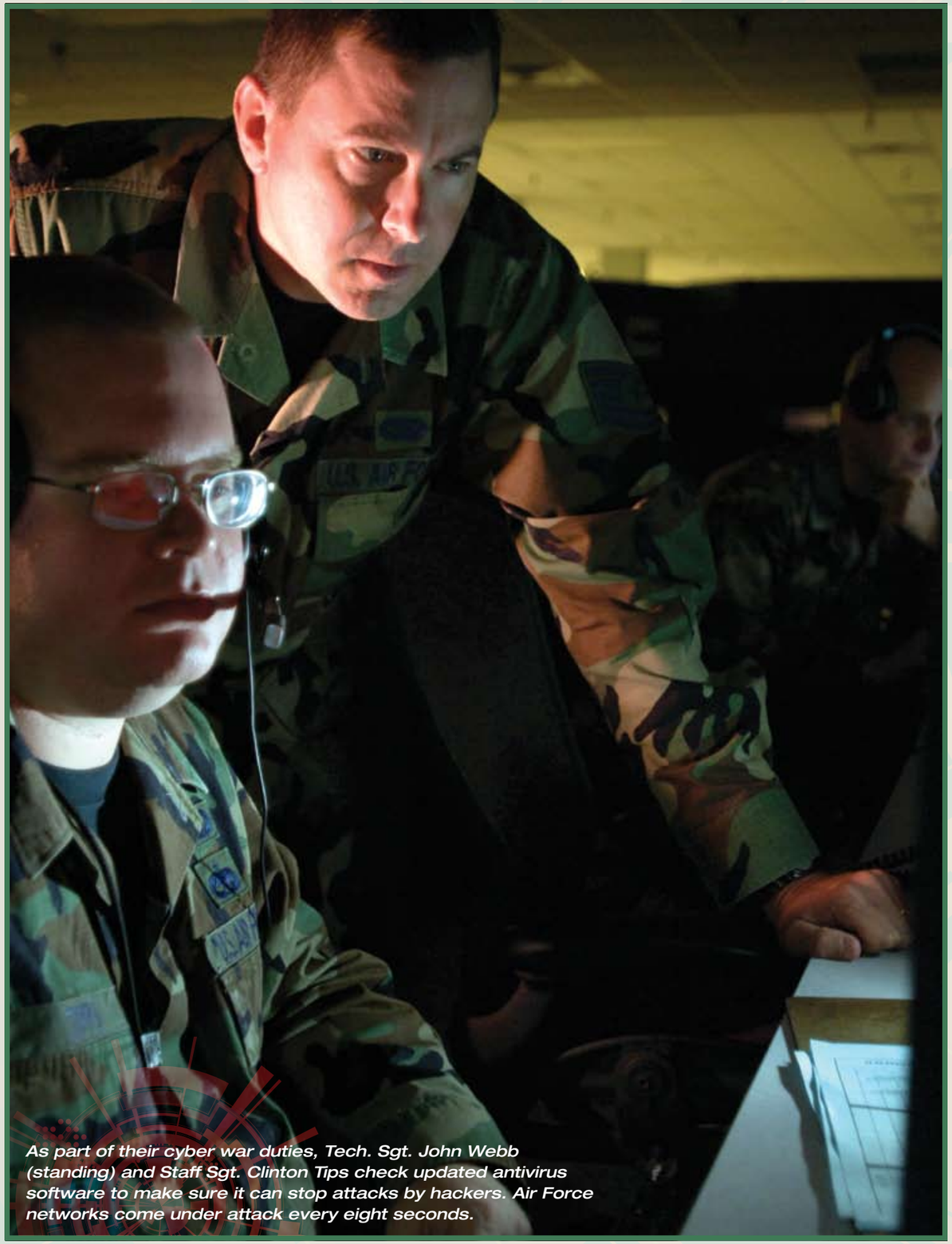
DECIPHERING CYBERSPACE

AIRMEN FENDING OFF ATTACKS ON A NEW BATTLESPACE

by Staff Sgt. Matthew Rosine
photos by Tech. Sgt. Cecilio Ricardo

To ensure bases across the United States have the latest tools to fight cyberspace attacks, Tech. Sgt. John Webb calls each one when he sends them updated antivirus software.



As part of their cyber war duties, Tech. Sgt. John Webb (standing) and Staff Sgt. Clinton Tips check updated antivirus software to make sure it can stop attacks by hackers. Air Force networks come under attack every eight seconds.

The enemy is attacking — again.

The relentless attack cascades across the base's sturdy defenses every few seconds. Staff Sgt. Carlos Miranda responds, his fingers dancing across his computer keyboard.

The relentless onslaught is business as usual for the sergeant, a 33rd Network Warfare Squadron network defense crewmember at Lackland Air Force Base, Texas. A member of the Air Force's Network Security Division, he watches and responds to a barrage of probes, malicious code and attempted breaches of Air Force networks.

The sergeant isn't fighting a battle in some far-off dusty desert. He fights his battles from an operations center, where the smell of coffee fills the air. No matter. He and his crewmembers must ensure critical data and networks are available to support Air Force operations worldwide.

That's a tall order. But the sergeant and the other members of his highly trained crew, a mix of Airmen and Air Force civilians and contractors, know their job well.

Airmen fighting the war on terrorism around the globe may not realize it, but they depend on the Lackland crew to complete their missions.

It's a never-ending battle. One the Air Force is determined to win.

"We estimate our network operations people see an alert of some kind every eight seconds," said Lt. Gen. Robert J. Elder Jr., commander of 8th Air Force and the joint functional component commander for global strike and integration for U.S. Strategic Command.

"We thwart most attacks through a number of measures we have implemented on Air Force systems," the general said. "When one gets through, we work with partners in intelligence and law enforcement to do the forensics analysis that tells us where it came from, and how to stop the next one from affecting our ability to operate effectively across the globe."

The team ensures critical data and networks are available to support all Air Force operations. That could be a tanker airlift control element in Europe, a medical unit in Southwest Asia, a forward supply area in South America or intelligence analysts awaiting imagery downloads.

All these missions rely on the connectivity that enables them to pass mission critical data — tanker tracks and schedules over the Pacific, patient data, critical spares shipment information and even air tasking orders.

This data and the networks and systems it resides on are under constant, deliberate attack.

Dominating a domain

The cyberspace war affects every part of the Air Force mission. But while Air Force cyber experts understand the importance of the cyberspace battlefront, most Airmen still wonder, "What exactly is cyberspace?"

In simplest terms, it is any electronic signal or anything that sends, receives or reflects those signals. For the warfighter, it is a new medium for military operations. And in an era where almost every Airman has access to, or can transmit, data, cyber security is paramount.

"It is important for every Airman to recognize the Air Force approach to cyberspace is that it is a warfighting domain, just like air and space," General Elder said. "We intend to dominate that domain, and use it to provide sovereign options for the nation and battlefield effects for joint force commanders.

Cyberspace is not just a computer on someone's desktop, or a "virtual reality" game. It is another way the Air Force intends to fly and fight, he said.

With cyberspace integrated with the Air Force's already robust air and space operations, "it's a triple threat for the bad guys," the general said.

"Cyberspace operations are not and will not be a secondary competency for the Air Force," he said. "Cyber ops are tightly integrated with every aspect of modern military operations."

That is why the cyber command is building a strong foundation for future cyber warriors. The focus is on training, crew certifications and a diverse set of skills that span and transcend current specialties in communications, intelligence, operations and command and control.

The cyber command mission is to provide global effects in cyberspace, General Elder said. And the first thing the Air Force must do is establish the cyber domain and operate it.

"I tell my pilot friends that if they want to go have some sort of air fight, they don't have to worry about if there will be air," the general said. "If someone wants to conduct operations in cyberspace — whether we're fighting in cyberspace itself, or using it in support of the air fight — the first thing we have to do is create the domain that we are going to fight in."

Delivering and sustaining cyberspace is a huge job. It needs the constant support of hundreds of Airmen, civilians and contractors to ensure AF networks are available, reliable and secure.

"Right now we're pretty much limited to the NIPR (non-classified Internet protocol router) and SIPR (secret Internet protocol router) nets," General Elder said. "But we envision our role expanding to incorporate some airborne and space networks in the future as we further integrate Air Force systems and capabilities."

At the local levels, Airmen will see cyber "safety" and risk management programs adapt to meet the needs of future operations. Anyone who uses a land line or cellular telephone, computer — even a personal digital assistant — is using cyberspace.

"No matter what job you're doing as an Airman, you're using cyberspace every day. Without it, you couldn't do your job," the general said.

Defending cyberspace

However, defending a medium with so many diverse aspects and uses is one of the many unique challenges facing cyber Airmen. The Air Force currently secures the domain, but it doesn't defend it, the general said.

"If you're at Balad (Air Base, Iraq), because you're in a hostile area, you carry some sort of a sidearm so you can help defend your operation," he said. "If you're at a base in the United States, you don't do that because you're not coming under attack.

But that is a misconception, the general said.

"Because every Air Force base is under constant cyber attack," General Elder said.

And although certified and dedicated network defenders like Sergeant Miranda are on constant "patrol," some attacks slip through.

"We realize that we need to provide every Airman with a cyber sidearm," the general said. "We need to arm our Airmen with the knowledge and skills to recognize an attack and take those initial actions to shut it down."

Yet, even with the proper equipment, Airmen face a significant and ever-changing foe.

"People expect me to name some country. But I tell them one of the greatest threats to the Air Force network is the users on the Air Force network," General Elder said. "What we need to do is ensure our Airmen do not inadvertently attack their own network."

Unintended attacks can occur when Airmen download materials from unsafe Web sites, or use unsafe CDs or thumb drives on their government computer systems. This can allow viruses and worms into Air Force networks and make them unknowing accomplices to cyber terrorists.

Most Airmen are aware of the dangers of computer viruses that can destroy data. But they may not realize the increasing sophistication of the attack software residing invisibly on many internet sites or attachments.

"Once an Airman brings that code inside our defenses, it can signal an adversary with data about the system it's on, or even exfiltrate the data itself. That data compromise can put our Airmen's lives at stake," General Elder said.

Despite the many challenges they face, cyber command Airmen are excited about being at the forefront of tomorrow's Air Force — the front lines of the cyber war.

"Not only am I defending our Airmen and their operations as my normal job, but I'm also involved in a couple of extra projects that I not only find interesting, but a challenge," cyber warrior Staff Sgt. Erich Stoll said. He is a network battle manager at the Air Force Network Operations Center at Barksdale Air Force Base, La. It provides the command and control element integrating global Air Force network operations and defense.

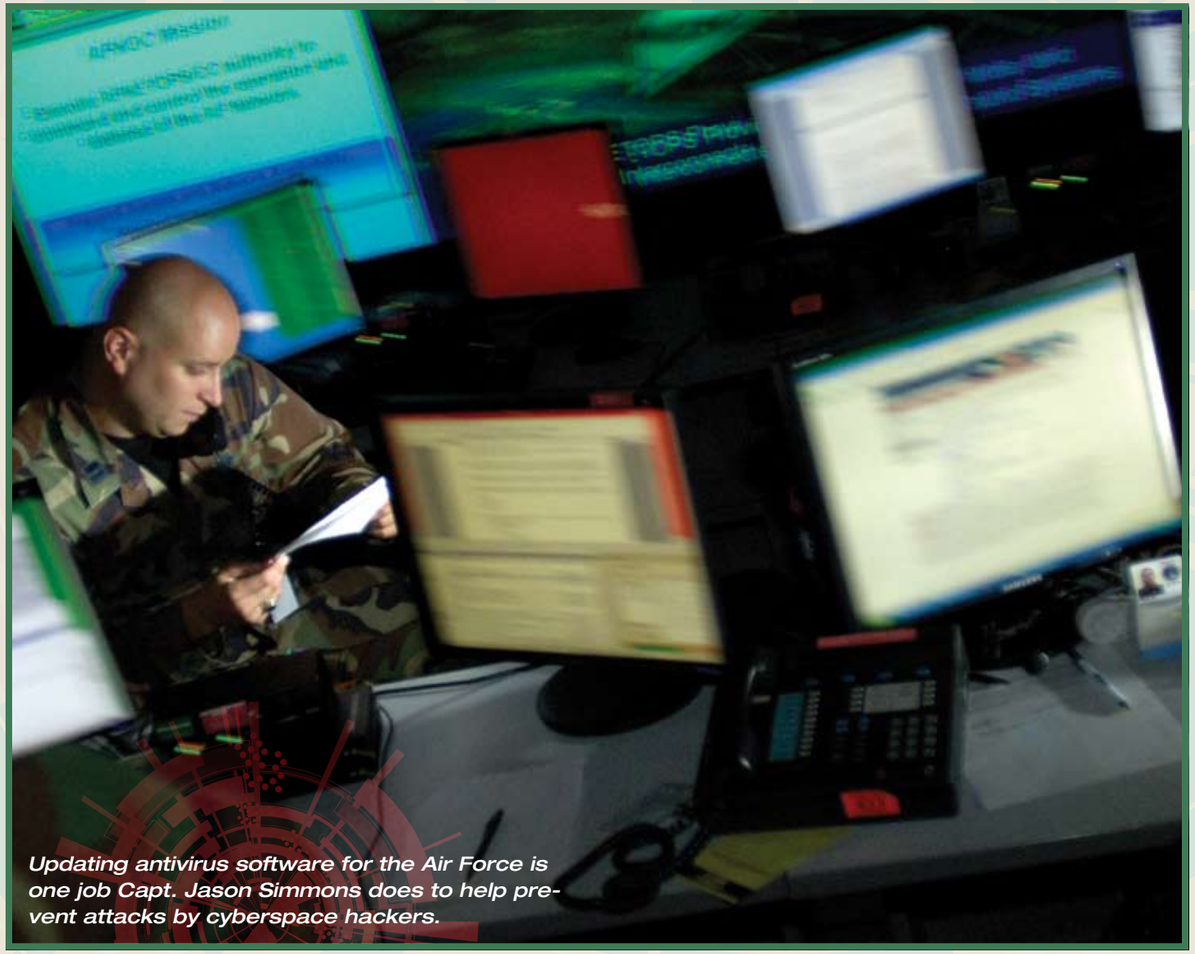
"It's very satisfying to me," Sergeant Stoll said.

At Lackland, Sergeant Miranda furiously taps at mambo-rhythm speed on his keyboard. He blocks a computer address that has repeatedly probed Air Force defenses. Mission accomplished. But he knows the attacker will probably change his address and try again.

No sweat, he and his crew are ready. But it's time to go. Another shift arrives to continue the cyber war. His team briefs the incoming crew on attacks and what may be developing trends.

Sergeant Miranda smiles and leans back into his well-worn computer chair.

"Man, I love my job," he said. "I really do."



Updating antivirus software for the Air Force is one job Capt. Jason Simmons does to help prevent attacks by cyberspace hackers.

How 'cyber' savvy are you?

Working in the realm of cyberspace means Airmen need to be cyber savvy. Are you? This quiz will let you know if you have what it takes to be a cyber warrior. *(Answer key at bottom of page.)*

1. What is a simple definition of cyberspace?
- a. The Internet
- b. A warfighting domain characterized by use of electronics and the electromagnetic spectrum
- c. The solar system

2. What is the AFNOC?
- a. Air Force Network Objectives in Cyberspace
- b. Armed Forces National Operations Center
- c. Air Force Network Operations Center

3. How many times each hour is there an alert in response to the Air Force network being attacked or probed?
- a. 82 (every 44 seconds)
- b. 164 (every 22 seconds)
- c. 450 (every 8 seconds)

4. What is one of the greatest threats to Air Force cyber operations?
- a. Air Force users
- b. Teen-age hackers
- c. Global warming

5. The AF Mission statement is: "Deliver sovereign options for the defense of the United States of America and its global interests — to fly and fight in air, space and _____."
- a. cyberspace
- b. with global dominance
- c. to infinity and beyond

6. How long has the Air Force been using cyberspace?
- a. Since Dec. 8, 2005 – The release of the new Air Force mission statement
- b. Since the release of the first laptop computer
- c. Since Air Force began using radios in aircraft

7. What kind of command is Air Force Cyber Command?
- a. an advanced technology command
- b. a warfighting command
- c. a support command

8. The Air Force will support _____'s mission in cyberspace
- a. USSTRATCOM
- b. USTRANSCOM
- c. USCYBERCOM

9. The Air Force's offensive cyberspace operations against its adversaries can range from:
- a. denial of service attacks to network hacking
- b. simple deterrence to complete destruction and defeat
- c. shock to awe

10. The military service committed to defend the Nation's cyberspace is _____
- a. The U.S. Air Force
- b. The U.S. Air Force
- c. The U.S. Air Force
- d. All of the above

Answer Key: 1. b, 2. c, 3. c, 4. a, 5. a, 6. c, 7. b, 8. a, 9. b, 10. d

How did you do?

You're **Cyber Savvy** if you answered 8 to 10 questions right. As a cyber warrior, feel free to inform others of your superior cyber knowledge.

If you answered 5 to 7 questions right, you're **Cyber So-So**. Good job, but you still have a little bit more to learn before you can become a true cyber warrior.

You're really **Cyber Sorry** if you only got 2 to 4 questions right. You have a lot to learn about cyberspace. You know all the answers now. So feel free take this quiz again — outscore your boss.

If you only got one right, you're a total **Cyber Loser**. Get on the stick and learn your role in the cyber war. The Air Force is counting on you.

Fighter and tanker operations rely on the secure connectivity cyber warriors provide them to pass on mission-critical data that allow them, and all Airmen around the globe, to do their jobs.

by Senior Airman Miranda Moore